AMENDMENTS TO THE CLAIMS (CLEAN VERSION)

Please amend the claims as follows.

1. (Currently Amended) A network system providing integration, comprising:

a remote access switch providing an interface between a client computer and a server, wherein all communications between the client computer and the server are transmitted via the remote access switch;

a client-side cryptographic function providing cryptographic services located on the client computer;

a server-side cryptographic function providing cryptographic services located on the server;

the client computer, configured to dial into the remote access switch, comprising:

a dial-up client for dialing the remote access switch; and

a custom script dynamically linked library providing an interface between the dial-up client and the client-side cryptographic function;

wherein the dial-up client is an executable file that loads and executes code in the custom script dynamically linked library;

the server, configured to connect to the remote access switch via a wide area network, comprising:

a PKI-Bridge providing an interface between the server and the server-side cryptographic function,

wherein the PKI-Bridge is configured to check version information of a client computer and send an identification to the server-side cryptographic function,

wherein the server-side cryptographic function is configured to generate a challenge string in response to the identification,

wherein the client-side cryptographic function is configured to generate a signed response string in response to the challenge string,

wherein the custom script dynamically linked library is configured to encode and divide the signed response string to obtain a plurality of packets,

wherein the PKI-Bridge is configured to combine and decode the plurality of packets to obtain a reconstructed signed response string,

wherein the server-side cryptographic function is configured to verify the reconstructed signed response string to generate a result, and

wherein the server-side cryptographic function is configured to send an instruction based on the result to the server via the PKI-Bridge, wherein the instruction specifies whether the server should send an allow connection message to the remote access switch.

2. (Previously Presented) The network system of claim 1, further comprising:

a security device holding authentication information; and

a security device reader attached to the client computer for reading the security device.

3. (Original) The network system of claim 2, wherein a certificate is stored on the security device.

4. (Original) The network system of claim 2, wherein the security device is a smart card.

5. (Original) The network system of claim 1, further comprising:

a directory service accessed by the server-side cryptographic function.

6. (Original) The network system of claim 5, wherein the directory service is lightweight directory access protocol compliant.

7. (Original) The network system of claim 1, wherein the client-side cryptographic function and the server-side cryptographic function employ the same cryptographic scheme.

8. (Previously Presented) The network system of claim 1, wherein the server-side cryptographic function uses a random number generator to generate the challenge string.

9. (Previously Presented) The network system of claim 1, wherein a client-side cryptographic function uses a random number generator to generate the signed response string.

10. (Cancelled)

11. (Cancelled)

12. (Cancelled)

13. (Original) The network system of claim 1, wherein the dial-up client operates in terminal mode.

14. (Currently Amended) A network system providing integration, comprising:

a remote access switch providing an interface between a client computer and a server, wherein all communications between the client computer and the server are transmitted via the remote access switch;

a client-side cryptographic function providing cryptographic services located on the client computer;

a server-side cryptographic function providing cryptographic services located on the server;

the client computer, configured to dial into the remote access switch, comprising:

a dial-up client for dialing the remote access switch; and

a custom script dynamically linked library providing an interface between the dial-up client and the client-side cryptographic function;

wherein the dial-up client is an executable file that loads and executes code in the custom script dynamically linked library;

the server, configured to connect to the remote access switch via a wide area network, comprising:

a PKI-Bridge providing an interface between the server and the server-side cryptographic function,

a security device holding authentication information;

a security device reader attached to the client computer for reading the security device; and

a directory service accessed by the server-side cryptographic function,

wherein the PKI-Bridge is configured to check version information of a client computer and send an identification to the server-side cryptographic function;

wherein the server-side cryptographic function is configured to generate a challenge string in response to the identification,

wherein the client-side cryptographic function is configured to generate a signed response string in response to the challenge string,

wherein the custom script dynamically linked library is configured to encode and divide the signed response string to obtain a plurality of packets,

wherein the PKI-Bridge is configured to combine and decode the plurality of packets to obtain a reconstructed signed response string,

wherein the server-side cryptographic function is configured to verify the reconstructed signed response string to generate a result; and

wherein the server-side cryptographic function is configured to send an instruction based on the result to the server via the PKI-Bridge, wherein the instruction specifies whether the server should send an allow connection message to the remote access switch.

15. (Currently Amended) A client computer comprising:

a dial-up client for dialing a remote access switch, wherein the dial-up client executes on the client computer, and wherein all communications between the client computer and a server are transmitted via the remote access switch;

a client-side cryptographic function providing cryptographic services located on the client computer; and

a custom script dynamically linked library providing an interface between the dial-up client and the client-side cryptographic function,

wherein the dial-up client is an executable file that loads and executes code in the custom script dynamically linked library,

wherein the client-side cryptographic function is configured to generate a signed response string in response to a challenge string from a server, and

wherein the custom script dynamically linked library is configured to encode and divide the signed response string to obtain a plurality of packets.

16. (Previously Presented) The client computer of claim 15, further comprising:

a security device reader attached to the client computer for reading a security device.

17. (Previously Presented) The client computer of claim 16, wherein the security device is a smart card.

18. (Previously Presented) The client computer of claim 15, wherein the custom script dynamically linked library comprises a SDLogin component and a SDSetupDial component.

19. (Original) The client computer of claim 15, wherein the dial-up client automates the authentication process using a hidden terminal operating in terminal mode.

20. (Currently Amended) A client computer comprising:

a dial-up client for dialing a remote access switch, wherein the dial-up client executes on the client computer;

a client-side cryptographic function providing cryptographic services located on the client computer; and

a custom script dynamically linked library providing an interface between the dial-up client and the client-side cryptographic function, and

a security device reader attached to the client computer for reading a security device,

wherein all communications between the client computer and a server are transmitted via the remote access switch;

wherein the dial-up client is an executable file that loads and executes code in the custom script dynamically linked library,

wherein the client-side cryptographic function is configured to generate a signed response string in response to a challenge string from a server, and

wherein the custom script dynamically linked library is configured to encode and divide the signed response string to obtain a plurality of packets.

21. (Currently Amended) A server configured to connect to a remote access switch via a wide area network, comprising:

a server-side cryptographic function providing cryptographic services located on the server; and

a PKI-Bridge providing an interface between the server and the server-side cryptographic function, wherein the PKI-Bridge is configured to check version information of a client and send an identification to the server-side cryptographic function;

wherein the server-side cryptographic function is configured to generate a challenge string in response to identification from the client,

wherein the PKI-Bridge is configured to combine and decode a plurality of packets to obtain a reconstructed signed response string which is a response to the challenge string,

wherein the server-side cryptographic function is configured to verify the reconstructed signed response string to generate a result;

wherein the server-side cryptographic function is configured to send an instruction to the server via the PKI-Bridge, wherein the instruction

specifies whether the server should send an allow connection message to the remote access switch based on the result, and

wherein all communications between the client and the server are transmitted via the remote access switch.

22. (Original) The server of claim 21, further comprising:

a directory service accessed by the server-side cryptographic function.

23. (Currently Amended) A server configured to connect to a remote access switch via a wide area network, comprising:

a server-side cryptographic function providing cryptographic services located on the server;

a PKI-Bridge providing an interface between the server and the server-side cryptographic function, wherein the PKI-Bridge is configured to check version information of a client and send an identification to the server-side cryptographic function; and

a directory service accessed by the server-side cryptographic function,

wherein the server-side cryptographic function is configured to generate a challenge string in response to identification from the client,

wherein the PKI-Bridge is configured to combine and decode a plurality of packets to obtain a reconstructed signed response string which is a response to the challenge string,

wherein the server-side cryptographic function is configured to verify the reconstructed signed response string to generate a result;

wherein the server-side cryptographic function is configured to send an instruction to the server via the PKI-Bridge, wherein the instruction specifies whether the server should send an allow connection message to the remote access switch based on the result; and

wherein all communications between the client and the server are transmitted via the remote access switch.

24. (Currently Amended) A method of integrating via a dial-up interface, comprising:

sending session initiation information from a dial-up client to a PKI-Bridge, wherein the dial-up client is an executable file that loads and executes code in a custom script dynamically linked library;

checking session initiation information by the PKI-Bridge;

generating a challenge string by a server-side cryptographic function in response to the session initiation information;

forwarding the challenge string to the custom script dynamically linked library;

forwarding the challenge string to a client-side cryptographic function from the custom script dynamically linked library;

utilizing a private key from a security device;

generating a response string in response to the challenge string;

signing the response string with the private key of a dial-in user to obtain a signed response string;

forwarding the signed response string to the custom script dynamically linked library;

encoding the signed response string to obtain an encoded signed response string;

dividing the encoded signed response string into a plurality of packets;

forwarding the plurality of packets to the PKI-Bridge;

combining the plurality of packets to obtain a reconstructed encoded signed response string;

decoding the reconstructed encoded signed response string to obtain a reconstructed signed response string;

forwarding the reconstructed signed response string to the server-side cryptographic function;

obtaining a public key of the dial-in user;

verifying the reconstructed signed response string based on the public key using the server-side cryptographic function to generate a result; and

sending an instruction to a server from the server-side cryptographic function via the PKI-Bridge, wherein the instruction specifies whether the server

should send an allow connection message to a remote access switch based on the result,

wherein the server is connected to the remote access switch via a wide area network;

wherein the dial-up client is configured to dial into the remote access switch; and

wherein all communications from the dial-up client and from the server are transmitted via the remote access switch.

25. (Previously Presented) The method of claim 24, further comprising:

reading the security device by a security device reader.

26. (Cancelled)

27. (Cancelled)

28. (Original) The method of claim 24, further comprising:

forwarding the challenge string to the dial-up client; and

forwarding the challenge string to the PKI-Bridge.

29. (Previously Presented) The method of claim 24, further comprising:

forwarding the plurality of packets from the custom script dynamically linked library.

30. (Original) The method of claim 24, wherein the security device is a smart card.

31. (Original) The method of claim 24, wherein the session initiation information comprises version information and a distinguished name.

32. (Original) The method of claim 24, wherein the public key is stored on a directory service.

33. (Original) The method of claim 32, wherein the directory service is lightweight directory access protocol compliant.

34. (Currently Amended) A method of integrating via a dial-up interface, comprising:

sending session initiation information from a dial-up client to a PKI-Bridge, wherein the dial-up client is an executable file that loads and executes code in a custom script dynamically linked library;

checking session initiation information by the PKI-Bridge;

generating a challenge string by a server-side cryptographic function in response to the session initiation information;

forwarding the challenge string to the custom script dynamically linked library;

forwarding the challenge string to a client-side cryptographic function from the custom script dynamically linked library;

utilizing a private key from a security device;

generating a response string in response to the challenge string;

signing the response string with the private key of a dial-in user to obtain a signed response string;

forwarding the signed response string to the custom script dynamically linked library;

encoding the signed response string to obtain an encoded signed response string;

dividing the encoded signed response string into a plurality of packets;

forwarding the plurality of packets to the PKI-Bridge;

combining the plurality of packets to obtain a reconstructed encoded signed response string;

decoding the reconstructed encoded signed response string to obtain a reconstructed signed response string;

forwarding the reconstructed signed response string to the server-side cryptographic function;

obtaining a public key of the dial-in user; and

verifying the reconstructed signed response string based on the public key using the server-side cryptographic function;

reading the security device by a security card reader;

forwarding the challenge string to the dial-up client;

forwarding the challenge string to the PKI-Bridge; and

forwarding the plurality of packets from the custom script dynamically linked library;

wherein the server is connected to a remote access switch via a wide-area network;

wherein the dial-up client is configured to dial into the remote access switch; and

wherein all communications from the dial-up client and from the server are transmitted via the remote access switch.

35. (Currently Amended) An apparatus of integrating via a dial-up interface, comprising:

means for sending session initiation information from a dial-up client to a PKI-Bridge, wherein the dial-up client is an executable file that loads and executes code in a custom script dynamically linked library;

means for checking session initiation information by the PKI-Bridge;

means for generating a challenge string by a server-side cryptographic function in response to the session initiation information;

means for forwarding the challenge string to the custom script dynamically linked library;

means for forwarding the challenge string to a client-side cryptographic function from the custom script dynamically linked library;

means for utilizing a private key from a security device;

means for generating a response string in response to the challenge string;

means for signing the response string with the private key of a dial-in user to obtain a signed response string;

means for forwarding the signed response string to the custom script dynamically linked library;

means for encoding the signed response string to obtain an encoded signed response string;

means for dividing the encoded signed response string into a plurality of packets;

means for forwarding the plurality of packets to the PKI-Bridge;

means for combining the plurality of packets to obtain a reconstructed encoded signed response string;

means for decoding the reconstructed encoded signed response string to obtain a reconstructed signed response string;

means for forwarding the reconstructed signed response string to the server-side cryptographic function;

means for obtaining a public key of the dial-in user;

means for verifying the reconstructed signed response string based on the public key using the server-side cryptographic function to generate a result; and

means for sending an instruction to a server from the server-side cryptographic function via the PKI-Bridge, wherein the instruction specifies whether the server should send an allow connection message to a remote access switch based on the result;

wherein the server is connected to the remote access switch via a wide area network;

wherein the dial-up client is configured to dial into the remote access switch; and

wherein all communications from the dial-up client and from the server are transmitted via the remote access switch.